Amendments to the specification:

Please amend the specification as follows:

Please insert the following headings:

Prior to paragraph [0001], please insert:

FIELD OF THE INVENTION

Prior to paragraph [0002], please insert:

BACKGROUND OF THE INVENTION

Prior to paragraph [0007], please insert:

SUMMARY OF THE INVENTION

Prior to paragraph [0018], please insert:

BRIEF DESCRIPTION OF THE DRAWINGS

Prior to paragraph [0029], please insert:

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS OF THE INVENTION

Please amend paragraphs [0010], [0033], [0050], [0060], [0061], [0062], [0071], [0085], [0094], [0095], [0098], [0112], and [0131]-[0135] as follows:

[0010] In another aspect, the present invention provides a method for encrypting digital data on an electronic device using an encryption key, the method comprising gathering session specific data; hashing said session specific data to obtain reference numbers referring to positions in an ~~authorization~~ authentication table stored in said electronic device; generating said encryption key from the characters stored in the ~~authorization~~ authentication table at said positions; and encrypting said digital data using said encryption key.

[0033] A random table is defined as a table comprising random numbers. Such a table may be created by suitable software as such. Alternatively, U.S. Patent ~~Application~~ No. 5,354,097, discloses another method of producing random numbers by optically scanning a randomly shaped material, such as a non-woven material. Likewise, a two-dimensional pattern may be used, which pattern has been formed by transformation of a bit string as disclosed in European Patent Application No. 1,219,088. From data collected during the reading of the randomly shaped material or pattern, random numbers can be derived, e.g., by using a predetermined algorithm.

[0039] As indicated in Fig. 1, the installation method for a new device for use with the tracking and tracing method according to the present invention starts with the generation of a random table, e.g. a table comprising randomly chosen characters or numbers, according to cell 2. The numbers may be generated using software employing an algorithm. Alternatively, as disclosed in U.S. Patent ~~Application~~ No. 5,354,097, random numbers may be deduced from a randomly shaped material, such as a non-woven material. For example, in a non-woven material, fibers are arranged in a random order due to the randomness of the production process. From the geometry of the fibers of the non-woven material numbers may be calculated. For example, a number that may be calculated, may be the angle between two fibers in an area of the material, or the number of fibers crossing an imaginary line. The calculated numbers will be random, as the geometry of the material is random. Another alternative manner, as disclosed in European Patent Application No. 1,219,088, to collect random numbers is by transforming a bit string into a two-dimensional pattern using an algorithm. As described above from this two-

dimensional pattern a table of random numbers may be calculated based on the geometry of the pattern.

[0050] When a connection with the TTP is established, the BIOS or authentication software sends its identification number upon request of the TTP according to cell 12. The TTP returns, possibly upon request of the BIOS, the ~~decrypt~~ decryption key, and the authentication software uses the ~~decrypt~~ decryption key according to cell 14 to generate an authentication table from the bit string which was embedded in the BIOS according to cell 8.

[0060] The authentication software and the bit string are put in a part of the BIOS which is accessible to the operating system ~~according to cell 28A~~. Next, according to cell 28B, the device needs to reboot to store the authentication software and the bit string in a secure part of the BIOS which is not accessible for the operating system.

[0061] At this point, the method continues as the method illustrated in Fig. 1 from cell 10 and further. According to cell 30 the device having newly stored authentication software and a bit string in its BIOS contacts the TTP again and requests a ~~decrypt~~ decryption key, for example the data string, according to cell 32.

[0062] According to cell 34, the ~~decrypt~~ decryption key is used to decrypt the authentication software and to decrypt the bit string and generate the corresponding authentication table. Next, according to cell 36, the authentication software verifies the authentication table and requests BIOS-specific data from the BIOS to encrypt the authentication table again.

[0071] A console 52 is an environment, which runs all the processes in the computer without user interruption. The console 52 plays an important role at start-up of the computer,

instructing the hardware devices 42 via the BIOS 44 to start and report their status. In case of errors, not only at start-up but also during operation, the BIOS 44 sends the error messages coming from the hardware 42 to the console 52. The console 52 then handles and corrects the errors. Thus, the console 52 runs the computer more or less stand-alone ~~the computer~~. A user may not interrupt or influence the console 52. Any instructions coming from the operating system 48 intended for the console 52 may therefore be blocked by the BIOS 44.

[0085] The authentication data are generated from a bit string that is generated at the device of the first transaction party and the bit string ~~and~~ is therefore not known to a second transaction party or a trusted third party (TTP). Thus, the second transaction party cannot generate and store (a copy of) the authentication data. For identification of the first transaction party in a transaction, the authentication data need to be known to the second transaction party or a TTP. Therefore, if the authentication data are to be used for identification in a transaction, a copy of the bit string is returned to the supplier of the authentication software package or to another party, which party may be a second transaction party or a TTP in accordance with cell 208.

[0094] Referring to Fig. 5A again, the application 50 may require a digital signature for an electronic transaction or for verification of legitimate use of digital data. Thereto, the authentication software 54 is executed to initiate decryption of the authentication data stored in memory location 63 and for generating said digital signature. From one authentication table, numerous digital ~~signs~~ signatures may be generated. Fig. 6 illustrates a method to generate a certain digital signature from an authentication table and illustrates how numerous different digital ~~signs~~ signatures may be generated. Using different digital ~~signs~~ signatures for every

action minimizes the chance of infringements or forgery and maximizes the ability to trace the origin of an illegal copy.

[0095] Fig. 6 shows two actors, a BIOS and the authentication software. The authentication software starts by collecting data according to cell 64. There are multiple components required. First a fixed component, which is identical for each instance a digital signature is generated. Further, a variable component is used, which enables the method to generate a numerous amount of different, but traceable digital ~~signs~~ signatures. A system trace component, e.g. a transaction ID, also depends on the instance. Two variable components make it virtually impossible to derive the authentication table from a number of generated digital ~~signs~~ signatures. Optionally, a personal identification number (PIN) or password may be used to identify the user as well as the device in which the authentication software is embedded.

[0098] Fig. 7 illustrates the track and trace method for digital files. Information contained in a digital file may be protected by copyrights, for example. Software, films or music may be bought and downloaded from the Internet. However, such digital files containing protected information may be very easily illegally copied and ~~spread~~ distributed without a trace of whom copied and ~~spread~~ distributed the file. Adding a trace in the digital file makes it possible to trace to origin of the illegal copy. Rightful owners of such a digital file, e.g. music file, will therefore not ~~spread~~ distribute the file, but they may use the file on different locations, for instance on their computer at home and on their portable digital player, e.g. MP3-player.

[0112] If the two digital ~~signs~~ signatures are identical, the application starts according to cell 110, otherwise the BIOS prevents the application being started, possibly informing the user that it is trying to use an illegal copy of the application.

[0131] In an even further embodiment, digital data may be encrypted using an encryption key that is generated according to the present invention, i.e. identical to the method for generating a digital signature. Fig. 6 illustrates how a digital signature may be generated according to the present invention by gathering session specific data, such as fixed data, variable data, personal data and/or device specific data. Hashing said session specific data may generate reference numbers, referring to positions in the ~~authorization~~ authentication table securely stored according to the present invention. Gathering the characters stored in the ~~authorization~~ authentication table at said positions generates a bit string comprising a number of characters. Said bit string may comprise any number of characters and said number may be dependent on the session specific data. Data encrypted with an encryption key having an unknown number of bits is virtually impossible to be cracked by another person not entitled to access said data.

[0132] To decrypt the data, the encryption key is required. To obtain the encryption key, the ~~authorization~~ authentication table and the session specific data are needed. Having an ~~authorization~~ authentication table stored and installed in a device according to the present invention, data may be securely stored in a memory of said device. The data may easily be decrypted when being accessed using said device. However, a copy of said encrypted data on any other device is rendered virtually inaccessible.

[0133] If identical ~~authorization~~ authentication tables are stored on two or more separate devices, encrypted data may be exchanged between said two or more devices. If the encrypted data are transferred from one device to another, together with the session specific data, the other device may regenerate the encryption key and decrypt the data. Such an encryption and

decryption method is especially useful for secure communication between said two or more devices over a publicly accessible network such as the Internet.

[0134] In an embodiment, a network server is provided with all ~~authorization~~ authentication tables of client devices connected to said server. A client attempting to access the server and the network of said server is authenticated by its digital signature, and thereafter all exchanged data may be encrypted using a digital signature. If a client sends data to another client, the data may be encrypted and transferred to the server together with the session specific data. The server decrypts the data using the session specific data and the ~~authorization~~ authentication table of the first client. Then, the server encrypts the data again, now using the ~~authorization~~ authentication table of the other client using the same or other session specific data. Next, the encrypted data are transferred to the other client together with the corresponding session specific data, which decrypts the data using its authentication ~~authorization~~ table.

[0135] Now referring to Fig. 10 again, the digital data securely stored on the portable and removable memory device may be an authentication ~~authorization~~ table according to the present invention. Thus, digital data encrypted using the ~~authorization~~ authentication table may be decrypted on any device when the portable and removable memory device is connected to said device and said device is provided with the ~~authorization~~ authentication software according to Fig. 10.

After paragraph [0135] and before the claims, please insert the following:

What is claimed is: